

No. 52544-5-II  
IN THE COURT OF APPEALS, DIVISION II  
OF THE STATE OF WASHINGTON

---

STATE OF WASHINGTON,

Respondent,

vs.

AARON MARK HARRIER,

Appellant.

---

FILED  
COURT OF APPEALS  
DIVISION II  
2019 MAY 16 PM 1:22  
STATE OF WASHINGTON  
BY MS  
DEPUTY

ON APPEAL FROM THE SUPERIOR COURT OF THE  
STATE OF WASHINGTON FOR CLARK COUNTY

The Honorable Bernard Veljacic, Judge

Clark County Superior Court Cause No. 16-1-01186-1

---

**APPELLANT'S OPENING BRIEF**

---

BRIAN A. WALKER  
Attorney for Appellant  
Brian Walker Law Firm, P.C.  
210 E. 22nd Street  
Vancouver, WA 98663  
[brian@walkerlawfirm.com](mailto:brian@walkerlawfirm.com)  
(360) 695-8886

<b><u>TABLE OF CONTENTS</u></b>	<b>Page</b>
1. TABLE OF CONTENTS.....	i
2. TABLE OF AUTHORITIES.....	i
3. ISSUE AND ASSIGNMENT OF ERROR.....	iii
4. STATEMENT OF THE CASE.....	1
5. ARGUMENT.....	4
6. CONCLUSION.....	18
7. CERTIFICATE OF SERVICE.....	18

<b><u>TABLE OF AUTHORITIES</u></b>	<b>Page</b>
<b><u>FEDERAL AND SUPREME COURT CASES</u></b>	
<i>Ex parte Jackson</i> , 96 U.S. 727.....	11
<i>Katz v. United States</i> , 389 U.S. 347, 88 S.Ct 507 .....	4
<i>U.S. v. Ackerman</i> , 831 F.3d 1292 (10th Cir. 2016).....	14
<i>U.S. v. Jacobsen</i> , 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85.....	8,9,13
<i>United States v. Tosti</i> , 733 F.3d 816, (Cir.2013).....	12,13,14
<i>Walter v. United States</i> , 447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 41 .....	9,11,12

<i>Wong Sun v. United States</i> , 371 U.S. 471, 83 S.Ct.407, 9 L.Ed.2d(1963) 441 .....	5,6
--	-----

#### STATE CASES

<i>Payton v. New York</i> , 445 U.S. 573, 589, 100 S.Ct. 1371, 1381-82, 63 L.Ed.2d 639 (1980).....	4
<i>State v. Boyer</i> , 102 P.3d 833, 124 Wn.App. 59 (Wash.App. Div. 3 2004).....	5
<i>State v. McKee</i> , 3 Wn.App.2d 11, 413 P.3d 1049, (Div. 1 2018) .....	7
<i>State v. Reid</i> , 98 Wn.App. 152, 988 P.2d. 1038 (1999).....	5
<i>State v. Rose</i> , 909 P.2d 280, 128 Wn.2d 388 (Wash 1996) .	5
<i>State v. Samalia</i> , 186 Wn.2d 262, 375 P.3d 1082, (2016)....	7
<i>State v. Simpson</i> , 95 Wn.2d 170, 622 P.2d 1199 1980).....	5
<i>State v. Smith</i> , 110 Wn.2d 658, 756 P.2d 722 (1988).....	6
<i>State v. Smith</i> , 36 Wn.App. 133, 672 P.2d. 759 (1983) .....	6
<i>State v. Trasvina</i> , 16 Wn.App. 519, 557 P.2d 368 (1976) .....	5
<i>State v. Young</i> , 123 Wash.2d 173, 867 P.2d 593 (1994).....	4,5

#### CONSTITUTIONAL PROVISIONS

Fourth Amendment, U.S. Constitution.....	4,13,15
--	---------

Washington State Constitution article I, section 7.....	5
---	---

### **ISSUE AND ASSIGNMENT OF ERROR**

Assignment of Error The Court erred by denying Defendant's motion to suppress the depictions discovered in this case as a result of a warrantless search.

#### Issue

Whether the warrantless search conducted by the investigating detective was illegal.

## **<sup>1</sup>STATEMENT OF THE CASE**

***(Unless otherwise indicated, the facts below are derived from CP 83, Pages 2-6)***

On December 31, 2015, Synchronoss Technologies, a cloud-based storage provider for Verizon Wireless customers, automatically scanned subscribers' stored data and located six images with hash values presumably matching hash values of previously known <sup>2</sup>child pornographic images. The scanning program Synchronoss used to scan the stored data, or whether it used a program at all, is unknown. How such program is designed and maintained is also unknown. Further, it is not known how the database of hash values, if any, used by Synchronoss for identifying known child pornographic images, was generated or maintained. The six images located by Synchronoss were not verified as being child pornographic images by a human being.

Synchronoss provided to the National Center for Missing and Exploited Children (NCMEC), a <sup>3</sup>CyberTip containing the six

---

<sup>1</sup> The facts set forth in this Statement of the Case are derived chronologically from Findings of Fact and Conclusions of Law entered following a trial on stipulated facts, CP 83, pages 2-6. Therefore, Clerk's Papers citations will be limited to one at the top of the Statement and the only other citations will be to Clerk's Papers other than the narrative facts in CP 83.

<sup>2</sup> The term "child pornography" is used variously herein in place of Washington's term, "depictions of minors engaged in sexually explicit conduct", to be consistent with the wording on the "CyberTip" referred to in this Brief, and for brevity. No casual reference or rewording to the Washington State legal definition is intended.

<sup>3</sup> "CyberTip" is the term of art used by the federally created agency National Center for Missing and Exploited Children (NCMEC) for an online referral of activity involving suspected child pornography.

unopened electronic image files, as required by federal statute, together with the subscriber's (Defendant's) telephone number associated with the account from which the six images were seized. The CyberTip was submitted on NCMEC's online form. Under "Incident Information" was the following information: "Incident Type: child pornography (possession, manufacture, and distribution)". CP 56, Exhibit 3, Page 8. There was no further information regarding the nature of the activity being reported in the CyberTip.

NCMEC did not open or in anyway view or compare the six image files, but forwarded the CyberTip with the six unopened images to law enforcement. Law enforcement ultimately placed the CyberTip together with the six unopened image files with Detective Jason Mills who is with the Vancouver Police Department (VPD), for follow up investigation.

Detective Mills opened and examined the six images without a warrant to confirm that the images appeared to be in fact depictions of children engaged in sexually explicit conduct.

Detective Mills then wrote detailed descriptions of each image and incorporated the descriptions into his application for a search warrant to be served upon Synchronoss and <sup>4</sup>Verizon Wireless. The search warrant was issued and directed Synchronoss and Verizon to provide information each company

---

<sup>4</sup> Synchronoss Technologies provides cloud based storage service to Verizon Wireless customers.

had which was associated with Defendant's account telephone number.

In response to the warrant, Synchronoss provided a thumb drive containing at least 10 more child pornographic images as well as Defendant's account information and a number of personal family photos and a photo of a wallet displaying Defendant's Washington State Driver's License.

The Verizon response included information which associated the Defendant's name with the account telephone number.

Based upon the information obtained from Synchronoss and Verizon pursuant to the initial warrant, Detective Mills obtained another warrant for the Defendant's residence and served it on May 31, 2016. At the residence, Defendant's cellular telephone was seized, analyzed and determined to be the device that had been used to download and then upload the images to the cloud.

The Defendant was detained and interrogated. During questioning, Defendant admitted to viewing, and then downloading to his cellular telephone the child pornographic images which had been discovered in his cloud-based storage as well as on his cellular telephone. There is no evidence that Mr. Harrier had been aware that images on his cell phone were being uploaded to the cloud storage.

## **ARGUMENT**

***When Detective Mills opened and examined the image files provided by Synchronoss without a warrant, he conducted an illegal search.***

The Fourth Amendment of the U.S. Constitution protects citizens from unreasonable searches and seizures and requires that all warrants be issued "upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. Warrantless searches and seizures inside a home are presumptively unreasonable. *Payton v. New York*, 445 U.S. 573, 586, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980).

The Fourth Amendment provides in part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...." In deciding whether an unconstitutional search has occurred, the court considers whether the defendant had a legitimate expectation of privacy and whether that expectation is one that society is willing to recognize as reasonable. *Katz v. United States*, 389 U.S. 347, 361, 88 S.Ct. 507, 516-17, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring); *State v. Young*, 123 Wash.2d 173, 189, 867 P.2d 593 (1994). A legitimate expectation of privacy is one which includes an actual and subjective expectation of privacy. *Katz*, 389 U.S. at 361, 88 S.Ct. at 516 (Harlan, J.,



concurring). "People have a reasonable expectation of privacy in their own homes." *Young*, 123 Wash.2d at 189, 867 P.2d 593 (quoting *Payton v. New York*, 445 U.S. 573, 589, 100 S.Ct. 1371, 1381-82, 63 L.Ed.2d 639 (1980)). *State v. Rose*, 909 P.2d 280, 128 Wn.2d 388 (Wash. 1996), *State v. Boyer*, 102 P.3d 833, 124 Wn.App. 593 (Wash.App. Div. 3 2004).

The Washington State Constitution article I, section 7, provides: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." Washington State's Constitution, article I, section 7, is explicitly broader than that of the Fourth Amendment as it "clearly recognizes an individual's right to privacy with no express limitations" and places greater emphasis on privacy. *State v. Young*, 123 Wn.2d 173, 180, 867 P.2d 593 (1994) (quoting *State v. Simpson*, 95 Wn.2d 170, 178, 622 P.2d 1199 (1980)).

In a motion to suppress evidence, a criminal defendant bears the initial burden of establishing that evidence was obtained unlawfully. *State v. Trasvina*, 16 Wn.App. 519, 557, 557 P.2d 368 (1976).

Once a prima facie case has been made that the search was illegal, the burden shifts to the State to establish that such evidence was obtained in a constitutionally sound manner. *State v. Reid*, 98 Wn.App. 152, 988 P.2d. 1038 (1999), *Wong Sun v. United States*,

371 U.S. 471, 83 S.Ct.407, 9 L.Ed.2d. 441 (1963). The burden is upon the State to show that the seizure of evidence was constitutionally sound by clear and convincing evidence. *State v. Smith*, 36 Wn.App. 133, 672 P.2d. 759 (1983).

Once a search has been determined to be illegal, all that which has been obtained thereby is deemed inadmissible as evidence. *Wong Sun v. United States*, 371 U.S. 471, 487-88,83 S. Ct. 407, 9 L. Ed. 2d 441 (1963) (evidence is inadmissible as the "fruit of the poisonous tree" where it has been obtained by illegal actions of the police). *State v. Smith*, 110 Wn.2d 658, 756 P.2d 722 (1988).

As time and technology has advanced, so has the law has in its steady fashion, finding that individuals have a reasonable expectation of privacy in cell phones.

Given the intimate information that individuals may keep in cell phones and our prior case law protecting that information as a private affair, we hold that cell phones, including the data that they contain, are "private affairs" under article I, section 7. As private affairs, police may not search cell phones without first

obtaining a warrant unless a valid exception to the warrant requirement applies.

*State v. Samalia* 186 Wn.2d 262, 375 P.3d 1082, (2016). See also *State v. McKee*, 3 Wn.App.2d 11, 413 P.3d 1049, (Div. 1 2018).

In this case, a police detective received six unopened files attached to a tip in an automated message from a company called Synchronoss Technologies. The tip simply indicated, "Incident Type: Child Pornography (possession, manufacture, and distribution)". The detective received no descriptions of the images, no information as to what Synchronoss Technologies is, and what, if any, verification had been performed regarding the six images. The detective then opened and viewed the six images.

The State may likely argue that the detective merely repeated the search that a private individual had already done where a warrant would not be required. This argument fails, however, as among the other reasons set forth below, the detective's search exceeded the scope of what Synchronoss was known to have done.

Though Appellant has found no Division II cases directly on point, there have been a number of instructive cases which are helpful in determining the direction of constitutional protection when private searches precede governmental searches.

In 1984, the U.S. Supreme Court found that a governmental search and field testing of an opened package of suspected

cocaine delivered to law enforcement by Fed Ex employees was a constitutional search. *U.S. v. Jacobsen*, 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85.

In *Jacobsen*, human being employees damaged a Fed Ex package with a forklift, opened the package to see if there was any damage, for insurance purposes and pursuant to a company policy. Inside, they found a pipe, or tube, made from duct tape. The employees cut the tube open and discovered a white powdery substance in a clear bag located at the center of the pipe. An agent arrived and repeated the unpackaging and saw the white, powdery substance in the clear bag. The agent extracted enough of the white powdery substance to perform a field test and found it to be presumptively cocaine. The Court found that the result of the private, Fed Ex search put the agent <sup>5</sup>lawfully in possession of the bag of white powder, without the need for a warrant. Ultimately, the Court noted that the field test that was conducted could only “reveal whether a substance is cocaine, and no other arguably ‘private’ fact”. *Jacobsen* at 124. In other words, even if the substance had turned out to be not cocaine, it would necessarily be merely some kind of white powder and nothing more — a fact which “reveals nothing of special interest”. *Id.*

---

<sup>5</sup> This holding has become to be known as the “private search doctrine”.

Unlike *Jacobsen*, no person had looked at the six images in our case and we can assume that a computer program scanned the hash values and automatically sent the CyberTip. To compare, had the Fed Ex employees been unjustifiably alarmed over a bag of what turned out to be, for example, talcum powder, there would be little offense to the privacy interests of the sender or recipient of the package. In our case, however, had the CyberTip been wrong, the images could have been innocent family photos that were among the Defendant's cloud storage, as in fact turned out to be the case, or legal photos of the Defendant engaging in sexual contact with another individual or some other private activity. It is this possibility that triggers the constitutional protection of a privacy interest in this case.

*Jacobsen* drew substantially for its reasoning from a 1980, U.S. Supreme Court case, *Walter v. United States*, 447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410. In *Walter*, a box containing 871<sup>6</sup> illegal pornographic 8-millimeter films was inadvertently delivered to the wrong company by the name of "L'Eggs" Products, Inc., rather than its intended recipient, "Leggs", Inc.. Employees of L'Eggs opened the box and found the illicit films. Though unable to view the films as they were without a projector, the employees noted that suggestive drawings appeared on one side of the film

---

<sup>6</sup> The films were homosexual pornography which, at the time, violated federal indecency laws.

container and a description of the illicit content of the films appeared on the other. Employees of L'Eggs called the FBI who's agents retrieved the box of films, observed the drawings and labeling just as the employees had, but then, without a warrant, went on to view a number of the films with a projector. The Supreme Court found the search performed by the police to be illegal.

[N]otwithstanding that the nature of the contents of these films was indicated by descriptive material on their individual containers, we are nevertheless persuaded that the unauthorized exhibition of the films constituted an unreasonable invasion of their owner's constitutionally protected interest in privacy. It was a search; there was no warrant; the owner had not consented; and there were no exigent circumstances. ...

To be sure, the labels on the film boxes gave them probable cause to believe that the films were obscene and that their shipment in interstate commerce had offended the federal criminal code. But the labels were not sufficient to support a conviction, ... . Further investigation -- that is to say,

a search of the contents of the films -- was necessary in order to obtain the evidence which was to be used at trial.

The fact that FBI agents were lawfully in possession of the boxes of film did not give them authority to search their contents. Ever since 1878, when Mr. Justice Field's opinion for the Court in *Ex parte Jackson*, 96 U.S. 727, established that sealed packages in the mail cannot be opened without a warrant, it has been settled that an officer's authority to possess a package is distinct from his authority to examine its contents.

When the contents of the package are books or other materials arguably protected by the First Amendment, and when the basis fr [sic] the seizure is disapproval of the message contained therein, it is especially important that this requirement be scrupulously observed.

Id at 655-7.

Though the present case does not involve a misdirected package, it does involve a fixed number of images which, as in

*Walter*, were arguably protected by the First Amendment. The detective here leapt to opening and viewing the images based upon a computerized tip containing merely the conclusory statement, "child pornography, possession, manufacture, and distribution" — far less than the drawings and detailed descriptions included in *Walter* which had been placed on the outside of the film containers by the owners themselves. It is also worth noting that the term "child pornography" is not a term used under Washington State law which prefers the less ambiguous term "depictions of minors engaged in sexually explicit conduct". There is actually no way to be sure that the term used in the CyberTip had the same meaning as required by Washington State law. We can only surmise that it was the word choice and judgment of a software writer or programmer.

Moving on to computer search cases, in 2013, the 9th Circuit found constitutional a police search of a laptop computer which followed a search conducted by a private citizen.. The search was repeated by the private citizen in the presence, and at the direction, of a police officer. Finding that the search was merely repeated just as the private citizen had done on his own, the Court found the search to be legal. *U.S. v. Tosti*, 733 F.3d 816 (9th Cir. 2013).



In *Tosti*, a CompUSA <sup>7</sup>store employee found thumbnail images of child pornography in the computer Tosti had dropped off for service. The employee contacted police and described the numerous images he had seen as containing naked adult men and children as well as graphic sex scenes involving children. The officer could see that the thumbnails were clearly child pornography, but had the employee enlarge the images and display them in a slide show so that they would be easier to view. The Court upheld the warrantless search, relying upon *Jacobsen*, saying,

The Fourth Amendment's proscriptions on searches and seizures are inapplicable to private action. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information. Instead, the Fourth Amendment is implicated only if the authorities use information with respect to which the

---

<sup>7</sup> Tosti's estranged wife several years later also turned over pornographic images believed to belong to Tosti to law enforcement, but that portion of the opinion dealt with apparent authority and consent searches and is not relevant to the matter herein.

expectation of privacy has not already been frustrated.

*United States v. Tosti*, 733 F.3d 816,822 (Cir. 2013).

The obvious and fundamental differences between *Tosti* and the present case is that in our case, there is no evidence that Mr. Harrier was aware that he had relinquished the contents of his cell phone to a third party as *Tosti* had and no private individual human was involved who had observed and reported in detail to police what he had seen. Moreover, the "repeat" of the search done presumably by a private party was in no way comparable to the hash value scan we assume the program did in our case. To the extent that Mr. Harrier's privacy interest may have been frustrated by some non-human action, no details were available upon which to base a determination that the images were in fact contraband, and the detective in the present case conducted his own, new search rather than direct another to repeat what that other had done privately. In this case, there was no way to know exactly what kind of search had taken place, or what had been observed.

In 2016, in a case perhaps more similar to the present one, *U.S. v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), the warrantless opening of an email was deemed illegal in an opinion authored by now U.S. Supreme Court Justice Neil Gorsuch. In *Ackerman*, America Online (AOL) software discovered images attached to an

email with hash values matching known contraband images. The known contraband images had been viewed in-house by trained, AOL employees who then catalogued the hash values into a database. However, when Ackerman's images were discovered by the AOL software, no employee opened and verified that the suspect images, except for a single image, were in fact a true match to prior, known contraband images. AOL sent an automated CyberTip to NCMEC where an analyst who processed the CyberTip opened and described not just the one verified by AOL, but all four attached images. The search was deemed illegal as it exceeded the scope of the AOL search by opening the email and image files. There, NCMEC was deemed a governmental agency and therefore, subject to the warrant requirement. The court found there that AOL had merely provided the unopened Image files in the attachment to NCMEC, but had not in fact opened the files. NCMEC's subsequent opening of the image files, the Court found, constituted an impermissible extension of the search done by AOL and was, therefore, an unlawful search.

In the present case, no assurances of reliability were present as in *Ackerman*, but the mere opening of the images constituted an impermissible expansion of the private search done by Synchronoss.

In all of the above cases, the searches by law enforcement were found to be illegal when determined to have exceeded the

scope of the search performed independently and prior by private individuals or companies. Further, the report of the suspected illegal activity was referred to law enforcement in most cases by human beings who had acted on their own who and could report their own observations. Moreover, in all of the cases, except the present one, it is established that a human being had either viewed the suspected contraband either before or after the private search occurred.

In this case, Synchronoss may have received automatic notice that one or more images with hash values matching one or more of those as being suspected "child pornography", had been uploaded to its cloud server by one of its subscribers. As required, Synchronoss provided the image files, unopened, to NCMEC via a CyberTip. The CyberTip itself did not include an open display of the image files from Synchronoss. This concluded the scope of the search performed by Synchronoss. Any further examination of the six image files was an expanded search performed by Detective Mills, a governmental agent.

Since a search of the images was illegal, any evidence obtained as a result thereof, including the evidence set forth in the detective's affidavit, was fruit of the poisonous tree. Therefore, the image descriptions he made of the images themselves and should have been suppressed. Further, since the detective used the

illegally obtained evidence to obtain subsequent search warrants, any such evidence should be suppressed as well as fruit of the poisonous tree.

Little information was known about Synchronoss Technologies at the time the detective reviewed the CyberTip. It was not, and is still not, known whether it was on the level of sophistication as are Google or Microsoft, or that it had been using a brilliant and reliable program for many years. Regardless, the time has not yet come that the law in the State of Washington has ceded the role of the neutral magistrate to a computer programmer's discretion.

A better, and legal, alternative to performing the warrantless search in the instant case would have been to apply for a warrant before opening the image files. No exigent circumstances were present and no other explanation has been given for the warrantless search other than perhaps inferred "convenience". A little inconvenience, however, is a small price to pay for protection of individual privacy rights as we continue further and irretrievably into the digital age.

With the proliferation of internet service providers, their subsidiaries and successors, there is substantial danger that the data age could devolve into a sort of digital wild west where private

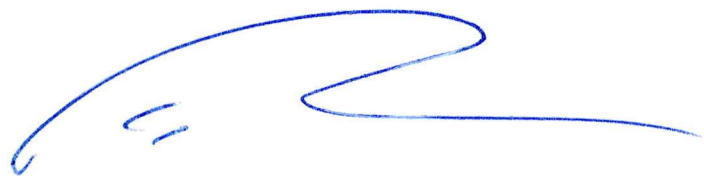
citizens and internet-based companies will determine the standards of our constitutional guarantee of privacy.

V. CONCLUSION

Police performed a warrantless search of six images provided by a private party who indicated that the images were suspected contraband images. The private party did not open or view the images or describe them. The police search exceeded the private search which occurred prior and therefore a warrant was required. All evidence in this matter was obtained as fruit of the poisonous tree and should be suppressed.

DATED this 13 day of May, 2019.

Respectfully Submitted:



---

BRIAN A. WALKER, WSBA # 27391  
Attorney for Defendant Harrier

**CERTIFICATE OF SERVICE**

I certify that on May 13, 2019, I provided a copy of the Appellant's Opening Brief by first class mail on the below-named, by mailing to said individuals copies thereof, contained in sealed envelopes, with postage prepaid, addressed to said individuals at said individuals' last known addresses as set forth below, and deposited in the post office at Vancouver, Washington on said day.

By way of United States Postal Service, First Class Mail to  
the Following:

RACHEL ROGERS, ATTORNEY FOR RESPONDENT  
CLARK COUNTY PROSECUTING ATTORNEY  
PO BOX 5000  
VANCOUVER, WA 98666

AARON HARRIER  
11328 NE 51ST CIRCLE # P150  
VANCOUVER, WA 98682

Dated this 13 day of May, 2019



YESENIA PIEDRA  
Legal Assistant

FILED  
COURT OF APPEALS  
DIVISION II  
2019 MAY 16 PM 1:22  
STATE OF WASHINGTON  
BY \_\_\_\_\_  
DEPUTY



BRIAN WALKER LAW FIRM, P.C.

BRIAN A. WALKER\*  
TRAVIS D. SPEARS\*\*

\*Licensed in Washington and Oregon  
\*\*Licensed in Washington and Idaho

May 13, 2019

Washington State Court of Appeals  
Division II  
950 Broadway, Ste 300  
Tacoma, WA 98402

RECEIVED

MAY 16 2019

CLERK OF COURT OF APPEALS DIV II  
STATE OF WASHINGTON

**Re: Aaron M. Harrier v. State of Washington**  
**Appeal No. 52544-5-II**

Dear Court Clerk:

Enclosed for filing please find the original Appellant's Opening Brief, pertaining to the above matter.

If you have any questions please do not hesitate to contact our office.

Sincerely,

Yesenia Piedra  
Legal Assistant to  
BRIAN A. WALKER  
Attorney at Law

:ycp